International Civil Aviation Organisation

Fifth Meeting of Aeronautical Telecommunication Network (ATN) Transition Task Force of APANPIRG

Phuket, Thailand, 9 – 13 June 2003

Agenda Item 4: Review the development status of ATN technical documents

Asia /Pacific ATN System Integrity Policy

SUMMARY

This paper is a revised outline draft of the Asia/Pacific ATN System Integrity Policy presented at the 7th Meeting of the ATNTTF Ad Hoc Working Group.

Asia/Pacific ATN System Integrity Policy

1. Purpose. This document prescribes the system integrity policy and associated requirements applicable to the Aeronautical Telecommunications Network (ATN) in the Asia/Pacific region. It applies to ATN implementations and defines the rules governing the protection of ATN services and resources (both equipment and information) associated with ATN applications and processes from both unintentional defects and deliberate attack. The design, implementation and operation of the ATN must support the complete and consistent enforcement of this system integrity policy.

2. Applicability. The ATN <<*….add high level description of ATN…*>> For the purpose of this policy, the ATN encompasses hardware, software, procedures, standards, facilities, and personnel. Security services provided in support of the ATN protect all data transmitted, stored, or processed by the system, for various levels sensitivity.

3. Authority. This document is published in accordance with the authority of the Asia and Pacific Regional Office of the International Civil Aviation Organization (ICAO).

4. Implementation and Enforcement. This system integrity policy defines a minimum set of rules to be enforced for the protection of data, services, and resources under ATN cognizance. Local authorities may apply more stringent rules or constraints, while not degrading the ATN system integrity posture and maintaining consistency with the minimum essential required system integrity rules identified in this ATN System Integrity Policy.

5. System Integrity Requirements. System integrity requirements apply to the protection of the physical information technology, the communications equipment, and the data and information systems. The protection of data involves all forms of data representation. (Note: The term "ATN data" is used to reference this type of information throughout the rest of this document.) Protection also applies to the facilities, environment, hardware, software, and people associated with the ATN.

a. Fundamental System Integrity Requirements. The fundamental ATN system integrity requirements are:

(1) Protect all ATN data directly associated with ATN applications and processes including ATN messages and directory information from unauthorized disclosure, modification, or deletion.

(2) Protect critical ATN services and resources from unauthorized use and denial of service.

(3) Verify the identity of appropriate users and processes that may cause actions to take place throughout the ATN.

(4) Establish accountability to individual person, organizational entity or process for events and actions taking place throughout the ATN.

b. System Integrity Services. Secure operation of the ATN depends upon the accurate and consistent enforcement of six high level services: confidentiality, data integrity, authenticity, availability, accountability, and interoperability.

(1) Confidentiality. Ensures data is not disclosed to unauthorized entities. For the ATN, confidentiality, when appropriate, extends to data associated with ATN support applications and processes including system management and security applications.

(2) Data Integrity. Ensures data has not been altered or destroyed in an unauthorized manner.

(3) Authenticity. Ensures that the source of data or the identity of an entity is as claimed.

(4) Availability. Ensures resources, services, and data are accessible and usable on demand or in a timely, reliable manner by an authorized entity.

(5) Accountability. Enables activities to be traced to users and processes that may then be held responsible for those actions. For ATN, accountability includes the security services of identification and authentication of data directly associated with ATN applications and processes and extends to ATN support applications.

(6) Interoperability. Ensures that ATN systems and procedures in the Asia/Pacific region are compatible and that they operate in a consistent and cohesive fashion,

c. System Integrity Policy Statements. Successful system integrity policy enforcement relies on the proper implementation and operation of the system integrity mechanisms and services.

(1) Functional Policy Statements

a. Identification and Authentication

(a) Users and processes shall be uniquely identified.

(b) Users and processes shall be authenticated before being granted access to ATN data, services, and resources.

.

<<Additional functional policy statements to be derived from Common Criteria Functional Requirements and an (updated) ATN Threat Assessment>>

.

x. Interoperability

(a) ATN systems shall be configured with unique addresses in accordance with the Asia/Pacific ATN Addressing Plan.

.

<<Additional functional policy statements to be derived from ATNTTF baseline documents>>

.

(2) Assurance Policy Statements

<<Assurance policy statements to be derived from Common Criteria Assurance Requirements>>

(3) Physical Security Policy Statements. Proper physical security is critical to all other system integrity services. The effectiveness of all technical security safeguards is based, in part, on the assumption, either explicit or implicit, that all components have adequate physical security protection. Applicable policy statements are:

(a) Automated information system and network hardware, firmware, and software used for ATN transmission, storage, or processing shall have adequate physical access controls commensurate with the sensitivity and value of the ATN information and the threats posed to those resources.

(b) ATN configuration items shall be protected from unauthorized modification or deletion.

(4) Training Policy Statements. Training is a basic component of the ATN system integrity strategy. All personnel involved with ATN must be trained to properly interact with ATN resources and services. Applicable policy statements are:

(a) Personnel shall be trained to use ATN and its system integrity features prior to initial access to ATN.

(b) ATN management and administrative personnel at all local and regional control centers shall receive training pertaining to ATN threats, vulnerabilities, and risks; ATN system integrity services, policies, and regulations; and ATN system integrity-related operational procedures.

(c) All personnel are required to successfully complete annual system integrity awareness training. Refresher training is required when personnel assume new or different duty responsibilities, when significant configuration changes occur that affect system integrity, or when different threats or new vulnerabilities are identified.

6. Certification and Accreditation. The process of conducting an evaluation of a system that produces the necessary information to entities responsible for deciding whether to place a system into operation is termed *certification*. The actual authorization by responsible entities to place a system into operation is termed *accreditation*.

<<Certification and Accreditation policy to be derived from

industry C&A processes and actual experience of Ad Hoc working group members>>

7. Approval Roles and Responsibilities. The following paragraphs provide a description of the roles and responsibilities of the Designated Approving Authorities (DAAs) involved in the ATN accreditation process.

a. Approval Process. To ensure that the ATN is operating in an acceptable manner ATN shall be formally accredited by cognizant DAAs issuing an approval to operate. Applicable policy statements are:

(1) The ATN shall be formally approved to operate by the cognizant DAAs.

(2) Significant changes to approved components, infrastructure, or enclaves will require another formal approval (or re-accreditation).

b. ATN Designated Approving Authorities.

(1) Regional DAA.

(2) State/Organization DAA.